Remarks:

The above application has been carefully reviewed in light of the first office action and the references cited and applied by the Examiner. The helpful comments of the Examiner are appreciated with regard to formal matters.

A new abstract has been submitted herewith to replace the original "Summary". Additionally, the corrections to the specification as suggested by the Examiner have been incorporated in this response.

With respect to the claims and in order to more clearly and distinctly set forth the differences over the prior art, original Claims 1, 3 and 5 have been replaced by a single new claim 13. Claims 7 and 9 through 12 inclusive have been replaced by a single new claim 14.

With regard to the original information disclosure statement, Applicant and counsel regret the inadvertent omissions that resulted in non-compliance with the rules. Additional information is set forth herein as a bona fide attempt to comply with 37 CFR §1.98. See 37 CFR §1.97(f) in this regard.

The original identification of the two German patents listed in the IDS is believed to be complete and additional copies thereof are attached.

The date of the "Design & Elektronik" publication is November 15, 1999 and the author appears to be Herbert Bernstein. The title of the article (a copy of which is attached) is b"Sicherheit im Internet - Verschlűsselungsverfahren".

The article from "Industrie-Elektrik & Elektonik" was published in the year 2000 and is reprinted from volume No. 4 of that year. The article (copy attached) was written by Frank J. Furrer and is entitled, "Offener Kanal fűr Wűhlmäuse".

Turning to the differences over the cited prior art and the references cited by the Examiner, Applicant is of the opinion that German Patent DE 198 51 709 is the closest reference. The known method provides a method for online updating of safety-critical software in the field of railroad signaling which allows an effective and simple cooperation of several participants compiling and checking product software as well as secure placing of this software in the target computer via unsecured communication channels.

The known prior art method provides a secure compilation, transfer and feeding-in of the software in the target computer with the participation of several participants. Each participant receives both a private and a public key whereby a certification entity is chosen by the participant for certifying the allocation of the keys to the participants and

whereby each participant receives his own key certificate and the certificate of the certification unit.

Thereafter each participant taking part in the compilation and checking of the product software signs with his/her secret key and the other signatures and the same are transmitted along with his own key certificate.

Furthermore, it is provided that the certification unit generates and signs for each case a list of examiners and that the product software along with the linked signature list and the list of the key certificates of the participants along with the list of examiners are fed to the target computer and are ultimately checked. Hence the product software is transmitted to the target computer and is checked there and which has been compiled and checked by a plurality of participants.

However, it will be noted that in this prior art a single participant is not allowed to change the state of the transmitted software or of the target computer. All that is checked is if the software as compiled and transferred corresponds to the conditions of the certification unit which does not provide for the active impact of the participants on the transferred data or the control apparatus. Further, the possibility of a software download of safety critical software is not mentioned.

In departing from the prior art teachings as noted above, the present invention is based on the development of a process for transferring data into or out of a control apparatus as changing the state of the control apparatus in the form of writing and reading data into and out of the apparatus exclusively by authorized persons and programs respectively.

This problem is solved by the inventive process set forth in new Claim 13 wherein, a memory range (BSS, PS, DS) of the memory-programmable control unit (16) is selectively acuatable through the coding of the data set to be transferred, that for changing the state of the memory-programmable control unit (16) in the form of reading (download) and writing (upload) of memory ranges (BSS, PS, DS) defined in the authorization list (28) user rights defined, user rights defined in the authorization list (28) are allotted to the at least one authorized person according to his individual sender identification (18,24), and that through the memory-programmable control unit (16) the data is provided with a digital signature when reading (downloading) data (10) from a memory range (BSS, PS, DS) protected in correspondence with the authorization list (28).

This invention is new and unobvious over German Patent DE 198 51 709 because user rights in the form of writing and reading in the storage area are allotted to the single authorized persons corresponding to an authorization list

stored in the control apparatus and because when downloading data from the SOPS, these are provided with a digital signal.

The present solution represents invention under the statute since none of the cited references, either taken alone or in combination teach the concept. German Patent DE 198 51 709 discloses a method for online updating of safety-critical software in a control apparatus utilizing a check list. According to page 3, lines 30-32, when receiving a new state of software, the safety computer checks the digital signatures of the examiner belonging to this state of software as well as the authorization of the examiner by means of the examiner lits when the examination is successful. Checking the authorization can only deal with the question of whether the examiner was generally entitled to check this software. The allocation of authorizations for changing the state of the control apparatus in the form of reading and writing data in storage areas also defined in the authorization list cannot be found in this reference. Neither does this patent refer to the download of software packages from a memory-programmable control unit.

The Examiner has rejected the claims on a combination of teachings from the US patent to Walker *et al.* (6,546,492) and the IBM publication "AS/40". Counsel and the Applicant respectfully traverse this rejection.

According to the two new parent claims 13 and 14, the invention contemplates the transfer of data into a memory-programmable control unit. In contrast to this, the known system deals with the actualization of software for a control unit via a network. For this purpose, a control unit, an identification server and an update server are provided. The control apparatus of the prior art is e.g. a PC card a PCMCIA card or a cell phone. This is only a software-update whereby a change of state of the PC card and the cell phone, respectively, is not approached by a file coded by an authorized person.

The IBM AS/400 publication enables the user to protect objects by using authorizations and authorization lists. The system demands additionally, that users have special privileges for access by means of orders to specified objects.

This deals with a system of access authorization for specified objects, whereby an interrelationship between a file to be loaded into the system and a user is not made, though. Rather, this concerns a user-related safety system.

The process according to the present invention is also not reached by using the teaching known from IBM AS/400 combined into the system according to US Patent No. 6,546,492. Even if the control apparatus or the host PC that receives the control apparatus is provided with an authorization list according to IBM, access is allowed only to specified users,

but files can be loaded and/or amended that do not show an individual user ID.

Only due to the process according to the present invention, i.e to code a file such that it has both a user ID and a key, it is secured that after examination of this file in the memory-programmable control unit only an authorized person with the corresponding individual transmitter ID a change of state in the form of reading and writing is allowed. In contrast to the prior art, in the system according to the present invention, the file defines which actions can be performed by which user.

German Patent DE 690 28 226 T2 discloses an access authorization process for use against unauthorized manipulation. The mechanisms for controlling the access to programs, processes, or users to resources as defined by a computer system, an access matrix and their special embodiments such as access lists, capability lists as well as lock-key mechanisms are described therein.

A safety data transfer between user and computer system is not learned from DE 690 28 226 T2.

German Patent DE 198 34 863 A1, a copy of which is attached hereto, relates to a process for safety data transfer between a numerical control and a separated apparatus. In this disclosure, two processors are provided in the separated apparatus, each coding the data to be transferred, for

increasing the safety of the transfer. A data transfer from the numerical control into the input device is not described in the DE 198 34 863 A1. Also not mentioned is an authorization list included in the control unit, which enables only authorized persons or programs having a digital signature to gain access to the control unit. Rather, DE 198 34 863 A1 is based on the problem of providing a process for a preferably fast data transfer, which requires preferably less additional effort for configuring a safety data transfer between control unit and apparatus. No measures can be found in the documents, taken either alone or in combination for changing the state of the control in the form of reading (download) or writing (upload) of data in defined storage areas by authorized persons.

The article of H. Bernstein: "Sicherheit im Internet (security in the internet]", Design & Elektronik (DE) 21(1999, pages 1767, 1768, 1770, 1772) relates in general to a coding process for data to be transferred. In this context, different coding procedures as public-key-cryptography, symmetric coding and asymmetric coding are described. The article does not refer to the transfer of a coded file into a storage-programmable control unit.

The article by Frank J. Furrer "Offener Kanal für Wühlmäuse (Open channel for Root Voles)", Industrie-Elektrik & Elektronik (IEE), 45. Jg. 2000, No. 4, pages 90-93, relates to

networking via Ethernet in industrial automation. The article deals with the backup of data and programs against physical destruction, the safeguarding of resources as well as the protection of data and programs against offences via the communication systems. It is suggested that the access to a safety area of a network is controlled and prevented. Concrete measures for protection, however, are not mentioned.

The process according to this invention makes it possible so that only authorized persons are entitled to write/upload user programs in a predefined firmware-storage area. This allows the possibility to supply firmware e.g. via a file which then can be loaded without difficulties by an operator of the control apparatus. Since the signature loses its validity when a file is manipulated only the authorized actualization of the file can be loaded.

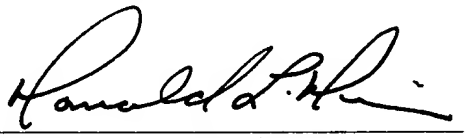
The process as described offers also the possibility to define program storage for an operator, in which the operator of a control apparatus can deposit parts of the program. Further areas of the program storage are defined according o the authorization list, so that these can be written only by the firmware producer and cannot be read by any other person.

Finally, the possibility is given to select data from storage-programmable controls which are provided with a digital signature so that a later manipulation of the data is prevented.

It is believed that the additional materials set forth above constitute the required information for the Information Disclosure Statement. In this regard the fee as specified in 37 CFR §1.17(p) is enclosed herewith ($180).

In view of the remarks and amendments above, it is now believed that the application is in condition for allowance and an early and favorable action is solicited.

Respectfully submitted,

By 

Donald L. Dennison
Reg. No. 19,920
Attorney for Applicant
Dennison, Schultz, Dougherty
& Macdonald
1727 King Street
Suite 105
Alexandria, VA 22314
(703) 837-9600 Ext. 15